CLAIMS

I claim:

1. A method of sending a digital message between a sender and a recipient in a public-key encryption scheme comprising the sender, the recipient and an authorizer wherein the digital message is encrypted by the sender and decrypted by the recipient, the method comprising:

(a) generating a recipient public key/ recipient private key pair; wherein the recipient private key is a secret of the recipient;

(b) generating a recipient encryption key;

(c) selecting a key generation secret that is a secret of the authorizer;

(d) generating a recipient decryption key using at least the key generation secret and the recipient encryption key, wherein a key formed from the recipient decryption key and a key formed from the recipient encryption key are a public key/ private key pair;

(e) encrypting the digital message using at least the recipient public key and the recipient encryption key to create an encrypted digital message; and

(f) decrypting the encrypted digital message using at least the recipient private key and the recipient decryption key.

2. The method of claim 1, wherein the recipient encryption key is generated from information comprising the identity of the recipient.

3. The method of claim 1, wherein the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key.

4. The method of claim 1, wherein the recipient encryption key is generated from information comprising the recipient public key.

5. The method of claim 1, wherein the recipient encryption key is generated from information comprising the identity of the recipient, the recipient public key, and a parameter defining a validity period for the recipient decryption key

6. The method of claim 1, wherein the recipient decryption key is generated by the authorizer according to a schedule known to the sender.

7. The method of claim 6, wherein the recipient encryption key is generated using at least information comprising the schedule.

8. The method of claim 1, wherein the recipient private key/ public key pair is generated using at least one system parameter issued by the authorizer.

9. The method of claim 1, wherein the recipient decryption key is generated by a method comprising:

(a) generating a first cyclic group $\mathbb{G}_1$ of elements and a second cyclic group $\mathbb{G}_2$ of elements;

(b) selecting a function $\hat{e}$ capable of generating an element of the second cyclic group $\mathbb{G}_2$ from two elements of the first cyclic group $\mathbb{G}_1$;

(c) selecting a generator P of the first cyclic group $\mathbb{G}_1$;

(d) selecting a random key generation secret s_C associated with and known to authorizer;

(e) generating a key generation parameter $Q = s_C P$;

(f) selecting a first function H_1 capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a first string of binary digits;

(g) selecting a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$;

(h) generating an element $P_B = H_1(\mathrm{Inf}_B)$, wherein Inf_B comprises a string of binary digits ; and

(i) generating a secret element $S = s_c P_B$ associated with the recipient; wherein the secret element is the recipient decryption key.

10. The method of claim 9, wherein Inf_B comprises the identity of the recipient, ID_{rec}, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

11. The method of claim 9, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

12. The method of claim 9 wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

13. The method of claim 9 wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

14. The method of claim 9 wherein:

s_C is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q is an element of the second cyclic group $\mathbb{G}_2$;

element P_B is an element of the first cyclic group $\mathbb{G}_1$;and

the secret element S is an element of the first cyclic group $\mathbb{G}_1$.

15. The method of claim 9, wherein the digital message M is encrypted by a method comprising:

generating the element P'_B = $H_{1'}(ID_{rec})$, wherein ID_{rec} comprises the identity of the recipient and wherein $H_{1'}$ is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

selecting a random key generation secret r; and

encrypting the digital message M to form a ciphertext C; wherein C is set to be:

$C = [rP, M \oplus H_2(g^r)]$, where $g = \hat{e}(Q, P_B)\hat{e}(s_BP, P'_B) \in \mathbb{G}_2$.

16. The method of claim 1, wherein the recipient encryption key is generated from a document and the recipient decryption key is the authorizer's signature on the document.

17. The method of claim 9, wherein the digital message M is encrypted by a method comprising:

generating the element $P'_B = H_{1'}(ID_{rec})$ wherein $H_{1'}$ is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

choosing a random parameter $\sigma \in \{0,1\}^n$;

set a random key generation secret $r = H_3(\sigma, M)$; and

encrypting the digital message M to form a ciphertext C; wherein C is set to be:

$C = [rP, M \oplus H_2(g^r), E_{H4(\sigma)}(M)]$, where $g = \hat{e}(Q, P_B)\hat{e}(s_BP, P'_B) \in \mathbb{G}_2$,

wherein H_3 is a function capable of generating an integer of the cyclic group $\mathbb{Z}/q\mathbb{Z}$ from two strings of binary digits, H_4 is a function capable of generating one binary string from another binary string, E is a secure symmetric encryption scheme, and $_{H4(\sigma)}$ is the key used with E.

18. A method of sending a digital message between a sender and a recipient in a public-key encryption scheme comprising the sender, the recipient and a plurality of authorizers, the plurality of authorizers including at least a root authorizer and *n* lower-level authorizers in a hierarchy between the root authorizer and the recipient, wherein $n \geq 1$, the method comprising:

(a) generating a recipient public key/ private key pair for the recipient; wherein the recipient private key is a secret of the recipient;

(b) generating a recipient encryption key using identity information of at least one of the recipient's ancestors;

(c) selecting a root key generation secret that is a secret of the root authorizer;

(d) generating a root key generation parameter based on the root key generation secret;

(e) generating a recipient decryption key such that the recipient decryption key is related to the recipient encryption key, the root key generation secret and the associated root key generation parameter;

(f) encrypting the digital message using the recipient public key and a recipient encryption key to create an encrypted digital message, wherein a key formed from the recipient decryption key and a key formed from the recipient encryption key are a public key/ private key pair; and

(h) decrypting the encoded digital message to recover the digital message using at least the recipient private key and the recipient decryption key.

19. The method of claim 18, wherein the recipient encryption key is generated from information comprising the identity of the recipient.

20. The method of claim 18, wherein the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key.

21. The method of claim 18, wherein the recipient encryption key is generated from information comprising the recipient public key.

22. The method of claim 18, wherein the recipient encryption key is generated from information comprising the identity of the recipient, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

23. The method of claim 18, wherein the recipient decryption key is generated according to a schedule known to the sender.

24. The method of claim 18, wherein the recipient private key/ public key pair is generated using system parameters issued by the authorizer.

25. The method of claim 18, wherein the recipient decryption key is related to the root key generation secret and the associated root key generation parameter.

26. The method of claim 18, wherein the plurality of authorizers further includes at least *m* lower-level authorizers in the hierarchy between the root authorizer and the sender, wherein $m \geq 1$, and wherein *l* of the *m* authorizers in the hierarchy are common ancestors to both the sender and the recipient, wherein authorizer is the lowest common ancestor authorizer between the sender and the recipient, and wherein $l \geq 1$, the method further

comprising:

selecting a lower-level key generation secret for each of the m lower-level authorizers in the hierarchy between the root authorizer and the sender; and

generating a sender decryption key such that the sender decryption key is related to at least the root key generation secret and one or more of the m lower-level key generation secrets associated with the m lower-level authorizers in the hierarchy between the root authorizer and the sender;

wherein the message is encrypted using at least sender decryption key and one or more of the lower-level key generation parameters associated with the $(m - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers above the lowest common ancestor authorizer$_l$; and

wherein the ciphertext is decrypted using at least the recipient decryption key and one or more of the lower-level key generation parameters associated with the $(n - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers that above the lowest common ancestor authorizer$_l$.

27. A method of generating a decryption key for an entity in an encryption system including a plurality of authorizers, the plurality of authorizers including at least a root authorizer and n lower-level authorizers in the hierarchy between the root authorizer and the entity, wherein $n \geq 1$, the method comprising:

generating a root key generation secret that is known to the root authorizer;

generating a root key generation parameter based on the root key generation secret;

generating a lower-level key generation secret for each of the n lower-level authorizers, wherein each lower-level key generation secret is known to its associated lower-level authorizer;

generating a lower-level key generation parameter for each of the n lower-level authorizers, wherein each lower-level key generation parameter is generated using at least the lower-level key generation secret for its associated lower-level authorizer;

establishing a decryption key generation schedule defining a validity period for a decryption key for the entity;

generating the decryption key for the entity such that the decryption key is related to at least the root key generation secret and one or more of the lower-level key generation secrets; and

providing the decryption key to the entity.

28. The method of claim 27, wherein the decryption key for the entity is related a parameter establishing a validity period.

29. A method of generating a decryption key for a recipient z in an encryption system, wherein the recipient z is n+1 levels below a root authorizer in the hierarchy, and wherein the recipient is associated with a recipient ID-tuple ($ID_{z1}, \ldots, ID_{z(n+1)}$) that includes identity information $ID_{z(n+1)}$ associated with the recipient and identity information ID_{zi} associated with each of n lower-level authorizers in the hierarchy between the root authorizer and the recipient, the method comprising:

generating a first cyclic group $\mathbb{G}_1$ of elements and a second cyclic group $\mathbb{G}_2$ of elements;

selecting a function $\hat{e}$ capable of generating an element of the second cyclic group $\mathbb{G}_2$ from two elements of the first cyclic group $\mathbb{G}_1$;

selecting a root generator P_0 of the first cyclic group $\mathbb{G}_1$;

selecting a random root key generation secret s_0 associated with and known to the root authorizer;

generating a root key generation parameter $Q_0 = s_0P_0$;

selecting a first function H_1 capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a first string of binary digits;

selecting a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$;

generating a element P_{zi} for each of the n lower-level authorizers, wherein $P_{zi} = H_1(\mathrm{ID}_1, \ldots, \mathrm{ID}_{zi})$ for $1 \leq i \leq n$;

selecting a lower-level key generation secret s_{zi} for each of the n lower-level authorizers, wherein each lower-level key generation secret s_{zi} is known to its associated lower-level authorizer;

generating a lower-level secret element S_{zi} for each of the n lower-level authorizers, wherein $S_{zi} = S_{z(i-1)} + s_{z(i-1)}P_{zi}$ for $1 \leq i \leq n$, *wherein* $S_0= Q_0$;

generating a lower-level key generation parameter Q_{zi} for each of the n lower-level authorizers, wherein $Q_{zi} = s_{zi}P_0$ for $1 \leq i \leq n$;

generating a recipient element $P_{z(n+1)} = H_1(\mathrm{ID}_{z1}, \ldots, \mathrm{ID}_{z(n)}, \mathrm{Inf}_{(n+1)})$ associated with the recipient, wherein $P_{z(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$ and wherein $\mathrm{Inf}_{(n+1)}$ is a string of binary digits ; and

generating a recipient decryption key $S_{zn+1} = S_{zn} + s_{zn}P_{zn+1} = \sum_{i=1}^{n+1} s_{zi-1}P_{zi}$ associated with the recipient.

30. The method of claim 29, wherein the recipient element $P_{z(n+1)} = H_1(\mathrm{ID}_{z1}, \ldots, \mathrm{ID}_{z(n+1)}, \mathrm{Inf}_{(n+1)})$ and wherein $\mathrm{Inf}_{(n+1)}$ comprises the identity of the recipient and a validity period for the identity-based decryption key.

31. The method of claim 29, wherein $\mathrm{Inf}_{(n+1)}$ further comprises a recipient public key generated by the recipient.

32. The method of claim 29, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

33. The method of claim 29, wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

34. The method of claim 29, wherein: the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

35. The method of claim 29, wherein:

s_0 is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q_0 is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation secrets s_{zi} is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each secret element S_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation parameters Q_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

the recipient element $P_{z\,(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

and

the recipient decryption key $S_{z(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$.

36. A method of encrypting and decrypting a digital message M communicated between a sender y and a recipient z in a hierarchical certificate-based encryption system, wherein the recipient z is n+1 levels below a root authorizer in the hierarchy, and wherein the recipient is associated with a recipient ID-tuple ($\mathrm{ID}_{z1}, \ldots, \mathrm{ID}_{z(n+1)}$) that includes identity information $\mathrm{ID}_{z(n+1)}$ associated with the recipient and identity information ID_{zi} associated with each of n lower-level authorizers in the hierarchy between the root authorizer and the recipient, the method comprising:

generating a recipient public key/ private key pair for the recipient; wherein the recipient private key is known to the recipient;

generating a first cyclic group $\mathbb{G}_1$ of elements and a second cyclic group $\mathbb{G}_2$ of elements;

selecting a function $\hat{e}$ capable of generating an element of the second cyclic group $\mathbb{G}_2$ from two elements of the first cyclic group $\mathbb{G}_1$;

selecting a root generator P_0 of the first cyclic group $\mathbb{G}_1$;

selecting a random root key generation secret s_0 associated with and known to the root authorizer;

generating a root key generation parameter $Q_0 = s_0P_0$;

selecting a first function H_1 capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a first string of binary digits;

selecting a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$;

generating an element P_{zi} for each of the n lower-level CAs, wherein $P_{zi} = H_1(\mathrm{ID}_1, \ldots, \mathrm{ID}_{zi})$ for $1 \leq i \leq n$;

selecting a lower-level key generation secret s_{zi} for each of the n lower-level authorizers, wherein each lower-level key generation secret s_{zi} is known to its associated lower-level authorizer;

generating a lower-level secret element S_{zi} for each of the n lower-level authorizers, wherein $S_{zi} = S_{z(i-1)} + s_{z(i-1)}P_{zi}$ for $1 \leq i \leq n$, *wherein* $S_{Z0} = Q_0$;

generating a lower-level key generation parameter Q_{zi} for each of the n lower-level authorizers, wherein $Q_{zi} = s_{zi}P_0$ for $1 \leq i \leq n$;

generating a recipient element $P_{z(n+1)} = H_1(\mathrm{ID}_{z1}, \ldots, \mathrm{ID}_{z(n)}, \mathrm{Inf}_{(n+1)})$ associated with the recipient, wherein $P_{z(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$ and wherein $\mathrm{Inf}_{(n+1)}$ is a string of binary digits;

generating a recipient secret element $S_{z(n+1)} = S_{zn} + s_{zn}P_{z(n+1)} = \sum_{i=1}^{n+1} s_{z(i-1)}P_{zi}$ associated with the recipient, wherein $\mathrm{Inf}_{(n+1)}$ comprises a validity period for the recipient secret element;

encoding the digital message to generate a ciphertext using at least the recipient public key, the root encryption parameter Q_0 and $Inf_{(n+1)}$; and

decoding the ciphertext C to recover the digital message M using at least the recipient private key, the lower-level key generation parameters Q_{zi} and the recipient secret element $S_{z(n+1)}$.

37. The method of claim 36 wherein: both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

38. The method of claim 36, wherein:

the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

39. The method of claim 36, wherein:

the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

40. The method of claim 36, wherein:

s_0 is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q_0 is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation secrets s_{zi} is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each secret element S_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation parameters Q_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

the recipient element $P_{z\,(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$; and

the recipient secret element $S_{z(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$.

41. The method of claim 36, wherein encoding the message M further comprises:

selecting a random parameter r; and

generating the ciphertext $C = [\text{rP}, V]$, wherein $V = M \oplus H_2(g^r)$, wherein

$$g=\hat{e}(P'_B,\ s_BP)\prod_{j=1}^{n+1}\hat{e}(P_j,\ s_{z(j-1)}P)$$

wherein s_BP is the recipient public key, P'$_B$ is $H_1(\text{Inf}_{(n+1)})$ and $Pj=H_1(s_{z(j-1)}P$, Inf(n+1)); and

decoding the ciphertext C further comprises:

recovering the digital message M from

$M = V \oplus H_2\ (\hat{e}(rP,\ S_{z(n+1)}))$.

42. The method of claim 36, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

43. The method of claim 36, wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

44. The method of claim 36, wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

45. The method of claim 36, wherein:

s_0 is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q_0 is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation secrets s_{zi} is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each secret element S_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation parameters Q_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

the recipient element $P_{z\,(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the recipient secret element $S_{z(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

r is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$; and

g is an element of the second cyclic group $\mathbb{G}_2$.

46. The method of claim 36, further comprising:

selecting a third function H_3 capable of generating an integer of the cyclic group $\mathbb{Z}/q\mathbb{Z}$ from a two strings of binary digits; and

selecting a fourth function H_4 capable of generating one binary string from another binary string;

wherein encoding the message M further comprises:

choosing a random parameter $\sigma \in \{0,1\}^n$;

set a random key generation secret $r = \mathrm{H}_3(\sigma, \mathrm{M})$; and

generating the ciphertext $C = [U_0, U_2, \ldots, U_t, V, W]$, wherein $U_0 = rs_BP$ *and* $U_i = rP_{zi}$ for $2 \leq i \leq n+1$, wherein $V = M \oplus H_2(g^r)$, and wherein $g = \hat{e}(Q_0, P_{z1})$ and s_BP is the recipient public key, wherein $g = \hat{e}(Q_0, P_{z1})$, and wherein $W = \mathrm{E}_{\mathrm{H}4(\sigma)}(\mathrm{M})$, E is a secure symmetric encryption scheme, and $\mathrm{H}_{4(\sigma)}$ is the key used with E; and

wherein decoding the ciphertext C further comprises:

recovering the random binary string σ using

$$\sigma = V \oplus H_2\left(\frac{\hat{e}(U_0, S_{z(n+1)})}{\prod_{i=2}^{n+1}\hat{e}(Q_{i-1}, U_i)}\right);\text{ and}$$

recovering the message M using $M = E^{-1}{}_{\mathrm{H}4(\sigma)}(\mathrm{W})$.

47. The method of claim 46, wherein both the first cyclic group $\mathbb{G}_1$ and the second cyclic group $\mathbb{G}_2$ are of the same prime order q.

48. The method of claim 46, wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

49. The method of claim 46, wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

50. The method of claim 46, further comprising authenticating the ciphertext C by:

computing an experimental random integer $r' = H_3(\sigma, M)$; and

confirming that $U_0 = r'P_0$ and $Ui = r'P_{zi}$ for $2 \leq i \leq n+1$.

51. The method of claim 46, wherein:

s_0 is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q_0 is an element of the second cyclic group $\mathbb{G}_2$;

each of the elements P_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation secrets s_{zi} is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each secret element S_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation parameters Q_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

the recipient element $P_{z\,(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the recipient secret element $S_{z(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

r is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$; and

g is an element of the second cyclic group $\mathbb{G}_2$.

52. The method of claim 26, wherein the plurality of authorizers further includes at least m lower-level authorizers in the hierarchy between the root authorizer and the sender y, wherein $m \geq 1$, wherein l of the authorizers in the hierarchy are common hierarchical ancestors to both the sender y and the recipient z, wherein $l \geq 1$, and wherein the recipient y is associated with a recipient ID-tuple $(\mathrm{ID}_{y1}, \ldots, \mathrm{ID}_{y(m+1)})$ that includes identity information $\mathrm{ID}_{y(m+1)}$ associated with the sender y and identity information ID_{yi} associated with each of K lower-level authorizers in the hierarchy between the root authorizer and the sender y, the method further comprising:

generating an element P_{yi} for each of the m lower-level authorizers, wherein $P_{yi} = H_1(\mathrm{ID}_{y1}, \ldots, \mathrm{ID}_{yi})$ for $1 \leq i \leq m$, and wherein $P_{yi} = P_{zi}$ for all $i \leq l$;

selecting a lower-level key generation secret s_{yi} for each of the m lower-level authorizers, wherein $s_{yi} = s_{zi}$ for all $i \leq l$;

generating a lower-level secret element S_{yi} for each of the m lower-level authorizers, wherein $S_{yi} = S_{y(i-1)} + s_{y(i-1)}P_{yi}$ for $1 \leq i \leq m$, and wherein $S_{yi} = S_{zi}$ for all $i \leq l$;

generating a lower-level key generation parameter Q_{yi} for each of the m lower-level CAs, wherein $Q_{yi} = s_{yi}P_0$ for $1 \leq i \leq m$, and wherein $Q_{yi} = Q_{zi}$ for all $i \leq l$;

generating a sender element $P_{y(m+1)} = H_1(\mathrm{ID}_{y1}, \ldots, \mathrm{ID}_{y(m+1)}, \mathrm{Inf}_{s(m+1)})$ associated with the sender y;

generating a sender secret element $S_{y(m+1)} = S_{ym} + s_{ym}P_{y(m+1)} = \sum_{i=1}^{m+1} s_{y(i-1)}P_{yi}$ associated with the sender; wherein $\mathrm{Inf}_{s(m+1)}$ comprises a validity period for the recipient secret element;

encoding the message M to generate a ciphertext C using at least the information comprising $\mathrm{Inf}_{(n+1)}$ and the lower-level key generation parameters Q_{yi} for $i \geq l$ and the sender secret element $S_{y(m+1)}$, but not using the lower-level key generation parameters Q_{yi} for $i < l$; and

decoding the ciphertext C to recover the message M using at least the recipient private key and the lower-level key generation parameters Q_{zi} for

$i \geq l$ and the recipient secret element $S_{z(n+1)}$, but not using the lower-level key generation parameters Q_{zi} for $i < l$.

53. The method of claim 52, wherein both the first cyclic group $\mathbb{G}_1$ and the second cyclic group $\mathbb{G}_2$ are of the same prime order q.

54. The method of claim 52, wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

55. The method of claim 52, wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

56. The method of claim 52, wherein:

s_0 is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q_0 is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{yi} is an element of the first cyclic group $\mathbb{G}$;

each of the lower-level key generation secrets s_{zi} is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each of the lower-level key generation secrets s_{yi} is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each secret element S_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each secret element S_{yi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation parameters Q_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation parameters Q_{yi} is an element of the first cyclic group $\mathbb{G}_1$;

the recipient element $P_{z(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the sender element $P_{y(m+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the recipient secret element $S_{z(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the sender secret element $S_{y(m+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

r is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$; and

g is an element of the second cyclic group $\mathbb{G}_2$.

57. The method of claim 52, wherein encoding the message M further includes:

selecting a random parameter r, and

encoding the message M to generate a ciphertext

$C = [U_0, U_{l+1}, \ldots, U_{n+1}, V]$, wherein $U_0 = rs_BP$ *and* $U_i = rP_{zi}$ for $2 \leq i \leq n+1$, wherein $V = M \oplus H_2(g^r)$, wherein $g = \hat{e}(Q_0, P_{z1})$, wherein s_BP is the recipient public key, and wherein $g_{yl} = \dfrac{\hat{e}(P_0, S_{y(m+1)})}{\prod_{i=l+1}^{m+1} \hat{e}(Q_{y(i-1)}, P_{yi})}$; and

decoding the ciphertext C further includes:

recovering the message M using $M = V \oplus H_2\left(\dfrac{\hat{e}(U_0, S_{z(n+1)})}{\prod_{i=l+1}^{n+1} \hat{e}(Q_{z(i-1)}, U_{zi})}\right)$.

58. A method of claim 57, wherein both the first cyclic group $\mathbb{G}_1$ and the second cyclic group $\mathbb{G}_2$ are of the same prime order q.

59. A method of claim 57, wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

60. A method of claim 57, wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

61. A method of claim 57, wherein:

s_0 is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q_0 is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{yi} is an element of the first cyclic group $\mathbb{G}$;

each of the lower-level key generation secrets s_{zi} is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each of the lower-level key generation secrets s_{yi} is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each secret element S_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each secret element S_{yi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation parameters Q_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation parameters Q_{yi} is an element of the first cyclic group $\mathbb{G}_1$;

the recipient element $P_{z\,(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the sender element $P_{y\,(m+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the recipient secret element $S_{z(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the sender secret element $S_{y(m+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

r is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$; and

g_{yl} is an element of the second cyclic group $\mathbb{G}_2$.

62. A method of claim 52, further comprising:

selecting a third function H_3 capable of generating an integer of the cyclic group $\mathbb{Z}/q\mathbb{Z}$ from a two strings of binary digits; and

selecting a fourth function H_4 capable of generating one binary string from another binary string;

wherein encoding the message M further comprises:

selecting a random binary string $\sigma \in \{0,1\}^n$;

computing a random integer $r = H_3(\sigma, M)$; and

generating the ciphertext $C = [U_0, U_{l+1}, \ldots, U_{n+1}, V, W]$,

wherein $U_0 = rs_BP$ *and* $U_i = rP_{zi}$ for $2 \leq i \leq n+1$, wherein $V = M \oplus H_2(g^r)$, wherein $g = \hat{e}(Q_0, P_{z1})$, wherein s_BP is the recipient public key and wherein $W =$ wherein $W = \mathrm{E}_{\mathrm{H4}(\sigma)}(\mathrm{M})$, E is a secure symmetric encryption scheme, and $\mathrm{H}_{4(\sigma)}$ is the key used with E, wherein $g_{yl} = \dfrac{\hat{e}(P_0, S_{y(m+1)})}{\prod_{i=l+1}^{m+1} \hat{e}(Q_{y(i-1)}, P_{yi})}$; and

wherein decoding the ciphertext C further comprises:

recovering the random binary string σ using

$$\sigma = V \oplus H_2\left(\frac{\hat{e}\left(U_0, S_{z(n+1)}\right)}{\prod_{i=l+1}^{n+1} \hat{e}\left(Q_{z(i-1)}, U_{zi}\right)}\right); \text{ and}$$

recovering the message M using $M = E^{-1}{}_{\mathrm{H4}(\sigma)}\ (\mathrm{W})$.

63. A method of claim 62, wherein both the first cyclic group $\mathbb{G}_1$ and the second cyclic group $\mathbb{G}_2$ are of the same prime order q.

64. A method of claim 62, wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

65. A method of claim 62, wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

66. A method of claim 62, wherein:

s_0 is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q_0 is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{yi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation secrets s_{zi} is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each of the lower-level key generation secrets s_{yi} is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each secret element S_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each secret element S_{yi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation parameters Q_{zi} is an element of the first cyclic group $\mathbb{G}_1$;

each of the lower-level key generation parameters Q_{yi} is an element of the first cyclic group $\mathbb{G}_1$;

the recipient element $P_{z\,(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the sender element $P_{y\,(m+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the recipient secret element $S_{z(n+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

the sender secret element $S_{y(m+1)}$ is an element of the first cyclic group $\mathbb{G}_1$;

r is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$; and

g_{yl} is an element of the second cyclic group $\mathbb{G}_2$.

67. A method of claim 62, further comprising:
authenticating the ciphertext C by:
computing an experimental random integer $r' = H_3(\sigma, M)$; and
confirming that $U_0 = r'P_0$ and $Ui = r'P_{zi}$ for $l+1 \leq i \leq n+1$.

68. A method of sending a digital message between a sender and a recipient in a public key encryption scheme comprising the sender, the recipient and a plurality of n authorizers, wherein $n \geq 1$ and wherein the recipient can decode the digital message only if the recipient possesses authorization from the authorizers, the method comprising:

generating a recipient public key/ private key pair for the recipient; wherein the recipient private key is a secret of the recipient;

generating a secret key s_i ($1 \leq i \leq n$) for each of the authorizers, wherein each key secret key is known to its associated authorizer;

generating a public key for each of the authorizers, wherein each public key is generated using at least the secret key for its associated authorizer;

generating a signature for each of the authorizers by signing a string of binary digits M_i with the secret key of that authorizer;

encrypting the digital message to form a ciphertext using at least the recipient's public key, the strings of binary digits M_i signed by the authorizers, and the public keys of the authorizers; and

decrypting the ciphertext using at least the recipient's private key and the signatures generated by the authorizers.

69. The method of claim 68, wherein at least one of the strings of binary digits is related to a parameter determining a validity period of the signatures generated by the authorizers.

70. The method of claim 69, wherein at least one of the strings of binary digits is generated from information comprising the identity of the recipient.

71. The method of claim 69, wherein at least one of the strings of binary digits is generated from information comprising the recipient public key.

72. The method of claim 67, further comprising:

generating a first cyclic group $\mathbb{G}_1$ of elements and a second cyclic group $\mathbb{G}_2$ of elements;

selecting a function $\hat{e}$ capable of generating an element of the second cyclic group $\mathbb{G}_2$ from two elements of the first cyclic group $\mathbb{G}_1$;

selecting a generator P of the first cyclic group $\mathbb{G}_1$;

selecting a key generation secret of an authorizer as s_i;

assigning the public key of an authorizer as s_iP;

selecting a first function H_1 capable of generating an element of the first cyclic group $\mathbb{G}_1$ from the string of binary digits M_i

generating a element P_{Mi} for each of the authorizers, wherein $P_{Mi} = H_1(s_iP,M_i)$ for $1 \leq i \leq n$; and

signing the element P_{Mi} to generate the signature $S_i = s_iP_{Mi}$ for each of the authorizers.

73. The method of claim 72, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

74. The method of claim 72, wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

75. The method of claim 72, wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

76. The method of claim 72, wherein each of the key generation secrets s_i is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each of the public keys S_i is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{Mi} is an element of the first cyclic group $\mathbb{G}_1$; and

the recipient private key s is an element of $\mathbb{Z}/\mathrm{q}\mathbb{Z}$.

77. A method of sending a digital message between a sender and a recipient in a public key encryption scheme comprising the sender, the recipient and a plurality of authorizers including at least a root authorizer and n lower-level authorizers in the hierarchy between the root authorizer and the recipient, wherein $n \geq 1$ and wherein the recipient can decrypt the digital message only if the recipient possesses authorization from the authorizers, the method comprising:

generating a recipient public key/ private key pair for the recipient, wherein the recipient private key is a secret of the recipient;

generating a secret key s_i for the root authorizer and each of the lower level authorizers, wherein each key secret key is known to its associated authorizer;

generating a public key for the root authorizer and each of the authorizers, wherein each public key is generated using at least the secret key for its associated authorizer;

certifying documents each comprising the public key of each of the lower level authorizers to generate a signature, wherein the document comprising the public key of each lower level authorizer is certified by the authorizer above it in the hierarchy;

certifying a document comprising the recipient public key, wherein the document is certified by the authorizer immediately above the recipient in the hierarchy;

encrypting the digital message to form a ciphertext using at least the recipient's public key and the public keys of the authorizers and the document; and

decrypting the ciphertext using at least the recipient's private key and the signatures generated by the authorizers.

78. The method of claim 77, wherein at least one of the public keys of the authorizers is related to a parameter determining a validity period of the signatures generated by the authorizers.

79. The method of claim 77, wherein at least one of the strings of binary digits is generated from information comprising the identity of the recipient.

80. The method of claim 77, wherein at least one of the strings of binary digits is generated from information comprising the recipient public key.

81. The method of claim 77, further comprising:

generating a first cyclic group $\mathbb{G}1$ of elements and a second cyclic group $\mathbb{G}2$ of elements;

selecting a function $\hat{e}$ capable of generating an element of the second cyclic group $\mathbb{G}_2$ from two elements of the first cyclic group $\mathbb{G}_1$;

selecting a generator P of the first cyclic group $\mathbb{G}_1$;

assigning the secret key of an authorizer as s_i;
assigning the public key of an authorizer as s_iP;

selecting a first function H_1 capable of generating an element of the first cyclic group $\mathbb{G}_1$ from the string of binary digits;

generating an element P_{Mi} for each of the lower level authorizers, wherein $P_{Mi} = H_1(s_iP, M_{i+1})$ for $1 \leq i \leq n-1$ and wherein M_{i+1} is related to the identity and public key of the authorizer immediately below that authorizer in the hierarchy; and

signing the elements P_{Mi} to generate the signatures $S_i = s_iP_{Mi}$.

82. The method of claim 81, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

83. The method of claim 81, wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

84. The method of claim 81, wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

85. The method of claim 81, wherein each of the key generation secrets s_i is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

each of the public key S_i is an element of the first cyclic group $\mathbb{G}_1$;

each of the elements P_{Mi} is an element of the first cyclic group $\mathbb{G}_1$; and

the recipient private key s is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$.

86. A method of encrypting and decrypting a digital message between a sender and a recipient in a public-key encryption scheme comprising the sender, the recipient and an authorizer wherein the digital message is encrypted by the sender and decrypted by the recipient, the method comprising:

(a) generating a recipient public key/ recipient private key pair; wherein the recipient private key is a secret of the recipient;

(b) selecting a key generation secret known to the authorizer;

(c) generating a recipient decryption key associated with time period i, wherein the recipient decryption key associated with time period i is related to the key generation secret, and wherein recipient decryption keys associated with time periods earlier than i, but not the recipient decryption keys associated with time periods later than i, can be generated from the recipient decryption key associated with time period i;

(d) encrypting the digital message to form a ciphertext using at least the recipient public key, the time period parameter associated with time period i or a time period parameter associated with an earlier time period, and a recipient encryption key to create an encrypted digital message; and

(e) decrypting the ciphertext using at least the recipient private key and the recipient decryption key associated with time period i.

87. The method of claim 86 wherein the recipient decryption key associated with time period i in related to information identifying the recipient.

88. A method of sending a digital message between a sender and a recipient in a public-key encryption scheme comprising the sender, a plurality of clients including the recipient, and an authorizer, wherein the digital message is encrypted by the sender and decrypted by the recipient, the method comprising:

(a) generating a recipient public key/ recipient private key pair for the recipient; wherein the recipient private key is a secret of the recipient;

(b) generating a unique binary string associating the recipient with a leaf node in a B-tree;

(c) generating an unique binary string associated with each ancestor node of the recipient leaf node;

(d) generating an encryption key for the recipient leaf node and for each of the ancestor nodes for the recipient leaf node, wherein the encryption key for each node is associated with at least the binary string associated with that node;

(e) generating a master secret known to the authorizer;

(f) generating a recipient decryption key associated with an ancestor node of the recipient leaf node, wherein the ancestor node is not an ancestor of a leaf node associated with a client not authorized by the authorizer, wherein the recipient decryption key is associated with at least the binary string associated with that node and the master secret, and wherein the recipient decryption key associated with an ancestor node of the recipient leaf node forms a private key/ public key pair with the encryption key associated with the ancestor node of the recipient leaf node;

(g) encrypting the digital message to create an encrypted digital message using at least the recipient public key, and the encryption keys associated with the recipient leaf node and ancestor nodes of the recipient leaf node; and

(h) decrypting the encrypted digital message using at least the recipient private key and the recipient decryption key associated with an ancestor node of the recipient leaf node.

89. The method of claim 88, wherein the encryption key for the recipient leaf node and for each of the ancestor nodes for the recipient leaf node are related to a validity period parameter defining a validity period for the decryption key associated with that node.

90. The method of claim 89, further comprising generating a long-lived certificate for the recipient, wherein the certificate comprises the recipient public key, the recipient serial number, wherein the recipient serial number is related to the binary string associating the recipient with the leaf node in a B-tree, and the validity period parameter.

91. The method of claim 88, wherein the nodes in the B-tree are associated with points on an elliptic curve or abelian variety.

92. The method of claim 88, wherein the binary string associating the recipient with a leaf node in a B-tree is generated by a method comprising:

choosing a binary string associated with the root node of the B-tree;

generating a binary string associated with each ancestor node of the recipient leaf node except for the root node, wherein the binary string associated with each ancestor node of the recipient leaf node except for the root node is generated using at least the binary string associated with the parent of that node; and

generating a binary string associated with recipient leaf node, wherein the binary string associated with the recipient leaf node is generated using at least the binary string of the parent of that node.

93. The method of claim 88, wherein the binary string associating the recipient with a leaf node in a B-tree is generated by a method comprising:

choosing the binary string associated with each recipient leaf node;

generating the binary string for the ancestor nodes of the recipient leaf node, wherein the binary string for each ancestor node of the recipient leaf node is generated using at least the binary strings associated with the child nodes of that node.

94. The method of claim 93, wherein the B-tree is a Merkle tree.

95. The method of claim 88, wherein the decryption key for the node providing cover for the recipient leaf node is generated by the method comprising:

(a) generating a first cyclic group $\mathbb{G}_1$ of elements and a second cyclic group $\mathbb{G}_2$ of elements;

(b) selecting a first function H_1 capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a first string of binary digits;

(c) generating an identifying string for the node providing cover for the for the recipient leaf node $P_{node} = H_1(\mathrm{Inf}_B)$, wherein Inf_B is related to the binary string associated with that node; and

(d) generating a secret element $S = s_c P_{\mathrm{node}}$ for each node; wherein the secret element S is the decryption key for the node providing cover for the for the recipient leaf node.

96. The method of claim 95, wherein the identifying string for the decryption key for the node providing cover for the recipient leaf node is also associated with the validity period parameter.

97. The method of claim 88, wherein the digital message is encrypted by a method comprising:

(a) generating a first cyclic group $\mathbb{G}_1$ of elements and a second cyclic group $\mathbb{G}_2$ of elements;

(b) selecting a function $\hat{e}$ capable of generating an element of the second cyclic group $\mathbb{G}_2$ from two elements of the first cyclic group $\mathbb{G}_1$;

(c) selecting a generator P of the first cyclic group $\mathbb{G}_1$;

(d) generating a key generation parameter $Q = s_c P$;

(e) selecting a first function H_1 capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a first string of binary digits;

(f) selecting a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$;

(h) generating an identifying string $P_{node} = H_1(\mathrm{Inf}_B)$ for each of m nodes defining the path from the recipient leaf node to the root node of the B-tree, wherein Inf_B is related to the binary string associated with that node;

selecting a random key generation secret r;

encrypting the digital message to form a ciphertext C; wherein C is set to be:

$C = [rP, V_1, \ldots, V_{m,}]$, where $V_i = M \oplus H_2(\hat{e}(P, P_{node\ i})^{rs_c})$, $\hat{e}(P, P_{node\ i}) \in \mathbb{G}_2$ and $P_{node\ i}$ is the identifying string associated with node i, i = 1, ..., m; and

encrypting a part of the ciphertext with the recipient public key PK_B.

98. The method of claim 97, wherein Inf_B is also associated with the validity period parameter.

99. The method of claim 97, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

100. The method of claim 97, wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

101. The method of claim 97, wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

102. The method of claim 98,wherein

s_C is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q is an element of the first cyclic group $\mathbb{G}_1$;

Identifying string P_{node} is an element of the first cyclic group $\mathbb{G}_1$; and the secret element S is an element of the first cyclic group $\mathbb{G}_1$.

103. A method of sending a digital message between a sender and a recipient in a public-key encryption scheme comprising the sender, a plurality of clients including the recipient, and an authorizer, wherein the digital message is encrypted by the sender and decrypted by the recipient, the method comprising:

(a) generating a recipient public key/ recipient private key pair for the recipient; wherein the recipient private key is a secret of the recipient;

(b) generating a binary string associated with the root node of the B-tree, wherein this binary string is related to a validity period parameter defining a validity period for a decryption key for a node providing cover for the recipient leaf node;

(c) generating a unique binary string associating the recipient with a leaf node in a B-tree;

(c) generating an unique binary string associated with each ancestor node of the recipient leaf node with the exception of the root node, wherein this binary string is associated with the position of its associated node in the B-tree;

(d) generating an encryption key for the recipient leaf node and for each of the ancestor nodes for the recipient leaf node, wherein the encryption key for each node is associated with at least the binary string associated with that node;

(e) generating a first master secret and a second master secret known to the authorizer;

(f) generating a decryption key for the node providing cover for the recipient leaf node, wherein the node providing cover for the recipient leaf node is not an ancestor node of a leaf node of a recipient not authorized to decrypt a message, wherein this decryption key is related to the first master secret, the second master secret x, and the binary strings associated with the node providing cover for the recipient leaf node and ancestor nodes of the node providing cover for the recipient leaf node and wherein the decryption key forms a private key/ public key pair with the encryption key associated with the node providing cover for the recipient leaf node;

(g) encrypting the digital message to create an encrypted digital message using at least the recipient public key, and the encryption keys associated with the recipient leaf node and ancestor nodes of the recipient leaf node; and

(h) decrypting the encrypted digital message using at least the recipient private key and the decryption key associated with the node providing cover for the for the recipient leaf node.

104. The method of claim 103, further comprising generating a long-lived certificate for the recipient, wherein the certificate comprises the recipient public key, the recipient serial number, wherein the recipient serial number is related to the binary string associating the recipient with the leaf node in a B-tree, and the validity period parameter.

105. The method of claim 103, wherein the B-tree is a Merkle tree

106. The method claim 103, wherein the binary string associating the recipient with a leaf node in a B-tree is generated by a method comprising:

choosing a binary string associated with a child of the root node of the B-tree;

generating a binary string associated with each ancestor node of the recipient leaf node except for the root node and the child of the root node, wherein the binary string associated with each ancestor node of the recipient leaf node except for the root node and the child of the root node is generated using at least the binary string associated with the parent of that node; and

generating a binary string associated with recipient leaf node, wherein the binary string associated with the recipient leaf node is generated using at least the binary string of the parent of that node.

107. The method claim 103, wherein the binary string associating the recipient with a leaf node in a B-tree is generated by a method comprising:

choosing the binary string associated with each recipient leaf node;

generating the binary string for the ancestor nodes of the recipient leaf node, with the exception of the root node, wherein the binary string for each ancestor node of the recipient leaf node, with the exception of the root node, is generated using at least the binary strings associated with the child nodes of that node.

108. The method claim 103, wherein the nodes in the B-tree are associated with points on an elliptic curve or abelian variety.

109. The method of claim 108, wherein the decryption key for the node providing cover for the recipient leaf node is generated by the method comprising:

(a) generating a first cyclic group $\mathbb{G}_1$ of elements and a second cyclic group $\mathbb{G}_2$ of elements;

(b) selecting a first function H_1 capable of generating a element of the first cyclic group $\mathbb{G}_1$ from a first string of binary digits;

(c) generating the identifying string for the root node in the B-tree $P_{mode} = H_1(\mathrm{Inf}_R)$ and wherein Inf_R is related to the validity period parameter;

(d) generating a secret element $S_R = s_c P_{mode}$ for the root node;

wherein the secret element S is the identity-based secret-key for the root node.

(e) generating the binary string associated with the node providing cover for the recipient leaf node and for each ancestor node of the node providing cover for the recipient leaf node, with the exception of the root-node, $P_{b1} \ldots P_{b1 \cdots bi}$, wherein the binary string associated with the node providing cover for the recipient leaf node and for each ancestor node of the node providing cover for the recipient leaf node is of the form $P_{node} = H_1(\mathrm{Inf}_B)$,

wherein Inf_B is related to the position of that node in the B-tree;

(f) generating a secret element:

$S = S_R + x(P_{b1} + \ldots + P_{b1 \ldots bi})$, xP for the node providing cover for the recipient leaf, wherein the secret element S is the decryption key for the node providing cover for the recipient leaf node.

110. The method of claim 103, wherein the digital message is encoded to create the encoded digital message by a method comprising:

(a) generating a first cyclic group $\mathbb{G}_1$ of elements and a second cyclic group $\mathbb{G}_2$ of elements;

(b) selecting a function $\hat{e}$ capable of generating an element of the second cyclic group $\mathbb{G}_2$ from two elements of the first cyclic group $\mathbb{G}_1$;

(c) selecting a generator P of the first cyclic group $\mathbb{G}_1$;

(d) generating a key generation parameter $Q = s_C P$;

(e) selecting a first function H_1 capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a first string of binary digits;

(f) selecting a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$;

(g) generating the identifying string for the root node in the B-tree $P_{rnode} = H_1(\text{Inf}_R)$, wherein Inf_R is related to the validity period parameter;

(h) generating the binary string associated with the recipient leaf node and for each ancestor node of the recipient leaf node, with the exception of the root-node, $P_{b1} \ldots P_{b1 \ldots bi}$, wherein the binary string the recipient leaf node and for each ancestor node of the recipient leaf node is of the form $P_{node} = H_1(\text{Inf}_B)$, wherein Inf_B is related to the position of that node in the B-tree;

(i) selecting a random key generation secret r;

(j) encrypting the digital message to form a ciphertext C; wherein C is set to be:

$C = [rP, rP_{b_1}, \ldots., r(P_{b_1} + \ldots + P_{b_1 \ldots b_m}), V]$, where $V = M \oplus H_2(\hat{e}(P, P_{rnode})^{rs}))$,

$\hat{e}(P, P_{rnode}) \in \mathbb{G}_2$; and

(k) encrypting a part of the ciphertext with the recipient public key PK_B.

111. The method of claim 110, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

112. The method of claim 110, wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

113. The method of claim 110 wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

114. The method of claim 110 wherein

s_C and x are elements of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q is an element of the first cyclic group $\mathbb{G}_1$;

Identifying strings P_{node} and P_{rnode} are elements of the first cyclic group $\mathbb{G}_1$; and

the secret element S is an element of the first cyclic group $\mathbb{G}_1$.

115. The method of claim 109, wherein the decryption key for the node providing cover for the recipient leaf node is updated to generate an updated decryption key, the method comprising:

(a) choosing a validity period for the updated decryption key;

(b) choosing a new value for the second master secret x; and

(c) generating the updated decryption key, wherein the updated decryption key is associated with an ancestor node of the recipient leaf node, wherein the ancestor node is not an ancestor of a leaf node associated with a client not authorized by the authorizer during the validity period for the updated decryption key,

wherein the updated decryption key is related to the first master secret s_C, the second master secret x, the new value for the second master secret x, and the binary strings associated with the ancestor node of the recipient leaf node and ancestor nodes of the ancestor node of the recipient leaf node and wherein the decryption key forms a private key/ public key pair with the encryption key associated with the ancestor node of the recipient leaf node.

116. The method of claim 115, wherein the updated decryption key is of the form:

$s_c(P_{T1} + P_{T2}) + x_1 P_{b1} + \ldots + x_m P_{(b1..bm)}$, wherein

s_c is the first master secret;

P_{T1} is the binary string associated with root node during the validity period of the decryption key;

P_{T2} is a binary string associated with root node during the validity period of the updated decryption key;

$x_1 \ldots x_m$ are associated with the second master secret and the new value for the second master secret; and

$P_{b1} \ldots P_{(b1..bm)}$, are the binary strings associated with node providing cover for the recipient leaf node during the validity period for the updated decryption key and the ancestor nodes of this node except for the root mode.